Configuring IP Utilities

Router Software Version 11.0
Site Manager Software Version 5.0

Part No. 114071 Rev. A
August 1996

Bay Networks

Bay Networks

4401 Great America Parkway
Santa Clara, CA 95054

8 Federal Street
Billerica, MA 01821

Copyright © 1988–1996 Bay Networks, Inc.

All rights reserved. Printed in the USA. August 1996.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Bay Networks, Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. A summary of the Software License is included in this document.

Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notice for All Other Executive Agencies

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Trademarks of Bay Networks, Inc.

ACE, AFN, AN, BCN, BLN, BN, BNX, CN, FN, FRE, GAME, LN, Optivity, PPX, SynOptics, SynOptics Communications, Wellfleet and the Wellfleet logo are registered trademarks and ANH, ASN, Bay•SIS, BCNX, BLNX, EZ Install, EZ Internetwork, EZ LAN, PathMan, PhonePlus, Quick2Config, RouterMan, SPEX, Bay Networks, Bay Networks Press, the Bay Networks logo and the SynOptics logo are trademarks of Bay Networks, Inc.

Third-Party Trademarks

All other trademarks and registered trademarks are the property of their respective owners.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Bay Networks, Inc. reserves the right to make changes to the products described in this document without notice.

Bay Networks, Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product are Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Bay Networks Software License

Note: This is Bay Networks basic license document. In the absence of a software license agreement specifying varying terms, this license -- or the license included with the particular product -- shall govern licensee's use of Bay Networks software.

This Software License shall govern the licensing of all software provided to licensee by Bay Networks ("Software"). Bay Networks will provide licensee with Software in machine-readable form and related documentation ("Documentation"). The Software provided under this license is proprietary to Bay Networks and to third parties from whom Bay Networks has acquired license rights. Bay Networks will not grant any Software license whatsoever, either explicitly or implicitly, except by acceptance of an order for either Software or for a Bay Networks product ("Equipment") that is packaged with Software. Each such license is subject to the following restrictions:

1. Upon delivery of the Software, Bay Networks grants to licensee a personal, nontransferable, nonexclusive license to use the Software with the Equipment with which or for which it was originally acquired, including use at any of licensee's facilities to which the Equipment may be transferred, for the useful life of the Equipment unless earlier terminated by default or cancellation. Use of the Software shall be limited to such Equipment and to such facility. Software which is licensed for use on hardware not offered by Bay Networks is not subject to restricted use on any Equipment, however, unless otherwise specified on the Documentation, each licensed copy of such Software may only be installed on one hardware item at any time.
2. Licensee may use the Software with backup Equipment only if the Equipment with which or for which it was acquired is inoperative.
3. Licensee may make a single copy of the Software (but not firmware) for safekeeping (archives) or backup purposes.
4. Licensee may modify Software (but not firmware), or combine it with other software, subject to the provision that those portions of the resulting software which incorporate Software are subject to the restrictions of this license. Licensee shall not make the resulting software available for use by any third party.
5. Neither title nor ownership to Software passes to licensee.
6. Licensee shall not provide, or otherwise make available, any Software, in whole or in part, in any form, to any third party. Third parties do not include consultants, subcontractors, or agents of licensee who have licensee's permission to use the Software at licensee's facility, and who have agreed in writing to use the Software only in accordance with the restrictions of this license.
7. Third-party owners from whom Bay Networks has acquired license rights to software that is incorporated into Bay Networks products shall have the right to enforce the provisions of this license against licensee.
8. Licensee shall not remove or obscure any copyright, patent, trademark, trade secret, or similar intellectual property or restricted rights notice within or affixed to any Software and shall reproduce and affix such notice on any backup copy of Software or copies of software resulting from modification or combination performed by licensee as permitted by this license.

9. Licensee shall not reverse assemble, reverse compile, or in any way reverse engineer the Software. [Note: For licensees in the European Community, the Software Directive dated 14 May 1991 (as may be amended from time to time) shall apply for interoperability purposes. Licensee must notify Bay Networks in writing of any such intended examination of the Software and Bay Networks may provide review and assistance.]
10. Notwithstanding any foregoing terms to the contrary, if licensee licenses the Bay Networks product "Site Manager," licensee may duplicate and install the Site Manager product as specified in the Documentation. This right is granted solely as necessary for use of Site Manager on hardware installed with licensee's network.
11. This license will automatically terminate upon improper handling of Software, such as by disclosure, or Bay Networks may terminate this license by written notice to licensee if licensee fails to comply with any of the material provisions of this license and fails to cure such failure within thirty (30) days after the receipt of written notice from Bay Networks. Upon termination of this license, licensee shall discontinue all use of the Software and return the Software and Documentation, including all copies, to Bay Networks.
12. Licensee's obligations under this license shall survive expiration or termination of this license.

Contents

Configuring IP Utilities

About This Guide

Before You Begin xvi
Conventions xvi
Acronyms xvii
Ordering Bay Networks Publications xviii

Technical Support and Online Services

Bay Networks Customer Service xx
Bay Networks Information Services xxi
World Wide Web xxi
Customer Service FTP xxi
Support Source CD xxii
CompuServe xxii
InfoFACTS xxiii
How to Get Help xxiii

Chapter 1
Starting TCP, FTP, Telnet, and NTP

Preparing a Configuration File 1-1
Configuring IP on a Circuit 1-2
Starting TCP 1-2
Creating TCP on a Router 1-2
Deleting TCP from the Router 1-3
Customizing TCP 1-3
Starting FTP 1-3
Creating an FTP Server on the Router 1-3
Deleting an FTP Server from the Router 1-4
Customizing FTP 1-4

Starting Telnet 1-4
Creating Telnet on the Router 1-4
Deleting Telnet from the Router 1-5
Customizing Telnet 1-5
Starting NTP 1-5
Creating NTP on the Router 1-5
Deleting NTP from the Router 1-6
Customizing NTP 1-6
Where to Go Next 1-6

Chapter 2
TCP, FTP, Telnet, and NTP Concepts

TCP Overview 2-1
How TCP Works 2-2
TCP Features 2-2
Connection Types 2-4
Connections and Connection States 2-4
TCP Memory Considerations 2-5
TCP and IP Service Users 2-6
FTP Overview 2-7
How FTP Works 2-8
Telnet Overview 2-10
How Telnet Works 2-11
Telnet Server 2-11
Telnet Client 2-12
NTP Overview 2-13
NTP Architecture 2-13
Distributing Time Throughout the NTP Network 2-14
Synchronizing with the Best Available Time Server 2-15
NTP Client Modes 2-15
Unicast Client Mode 2-15
Broadcast and Multicast Client Mode 2-16
Where to Go Next 2-17

Chapter 3
Customizing TCP Services

Configuring TCP on the Router 3-2
Enabling and Disabling TCP 3-2
Setting Minimum Retransmission Timeout 3-2
Setting Maximum Retransmission 3-3
Setting Maximum Window Size (bytes) 3-3
For More Information about TCP 3-3
Where to Go Next 3-4

Chapter 4
Customizing FTP Services

Configuring the FTP Server on the Router 4-1
Enabling and Disabling an FTP Server 4-2
Specifying the FTP Default Volume 4-2
Specifying Login Retries Value 4-2
Specifying Maximum FTP Idle Time 4-3
Specifying Maximum FTP Sessions 4-3
Specifying the Data Transmission Type 4-3
Specifying the FTP Control Connection 4-3
Specifying a Data Transfer Value 4-4
Specifying the TCP Window Size 4-4
Where to Go Next 4-4

Chapter 5
Customizing Telnet Services

Configuring a Telnet Server on the Router 5-1
Changing the Login Script Information 5-2
Changing the Name of the Manager's Login Script File 5-2
Changing the Name of the User's Login Script File 5-2
Enabling and Disabling User Logout 5-2
Changing the Telnet Configuration on the Router 5-3
Enabling and Disabling Telnet for the IP Router 5-3
Specifying the Maximum Number of Lines on the Technician Interface Console 5-3
Using the Pause Feature 5-3
Changing the Telnet Login Prompt 5-3
Changing the Login Timeout 5-4

Changing the Password Timeout 5-4
Changing the Command Timeout 5-4
Changing Login Retries 5-4
Using Telnet Server Diagnostics 5-5
Enabling Diagnostic Reporting 5-5
Enabling Diagnostic Exercise 5-5
Enabling Diagnostic Network Data 5-5
Enabling Diagnostic PTY Data 5-5
Enabling Diagnostic Options 5-6
Setting Technician Interface Login Scripts 5-6
Specifying a Filename for the Manager's Login Script 5-6
Specifying a Filename for the User's Login Script 5-6
Enabling and Disabling User Logout 5-6
Changing the History File 5-7
Configuring the Telnet Client on the Router 5-7
Enabling Telnet Client on the IP Router 5-7
Enabling Verbose Debug Logging 5-7
Changing the Remote Port 5-8
Changing the Command Prompt 5-8
Where to Go Next 5-8

Chapter 6
Customizing NTP Services

Configuring NTP on the Router 6-2
Enabling and Disabling NTP 6-2
Setting NTP Client Mode 6-2
Configuring Time Servers on a Router 6-2
Adding Time Servers 6-3
Setting Config Peer Mode 6-3
Setting Local Host Mode 6-4
Specifying the Source IP Address 6-4
Specifying Peer Preference 6-4
Deleting Time Servers from a Router 6-5
Configuring NTP Access Control 6-5
Adding Access Control to a Time Server 6-5
Specifying a Filter Type 6-5

Specifying an IP Subnet Mask 6-6
Deleting Access for a Time Server 6-6
Where to Go Next 6-6

Appendix A
Parameter Descriptions

TCP Global Parameters A-2
FTP Global Parameters A-4
Telnet Configuration Parameters A-7
Telnet Server Global Parameters A-8
Telnet Client Global Parameters A-14
NTP Global Parameters A-15

Appendix B
Site Manager Default Settings

TCP Parameters B-1
FTP Parameters B-2
Telnet Parameters B-3
NTP Parameters B-4

Index

Figures

Figure 2-1. TCP between IP and Clients 2-6
Figure 2-2. FTP Client and Server 2-8
Figure 2-3. Telnet Server 2-11
Figure 2-4. Telnet Client 2-12
Figure 2-5. Time Servers Forming a Synchronization Subnet 2-14
Figure 2-6. NTP Time Servers Operating in Unicast Client Mode 2-16

Tables

Table 2-1. TCP Reliability Features 2-3
Table 2-2. TCP Connection States 2-4
Table 2-3. FTP Commands Supported 2-9
Table B-1. TCP Configuration Parameters B-1
Table B-2. FTP Configuration Parameters B-2
Table B-3. Telnet Server Configuration Parameters B-3
Table B-4. Telnet Client Configuration Parameters B-3
Table B-5. NTP Configuration Parameters B-4

About This Guide

This guide describes how to configure the following IP utilities for your network: Transmission Control Protocol (TCP), File Transfer Protocol (FTP), Telnet, and Network Time Protocol (NTP).

If you are responsible for managing these utilities on Bay Networks™ routers or BNX® platforms, read this guide to see how to start up and customize these utilities on your network.

This guide offers

- A quick way to start TCP, FTP, Telnet, and NTP using default parameter values supplied in the software (Chapter 1)
- An overview and concepts behind TCP, FTP, Telnet, and NTP, to help you decide how to configure each protocol on your network (Chapter 2)
- Instructions for customizing TCP (Chapter 3)
- Instructions for customizing FTP (Chapter 4)
- Instructions for customizing Telnet (Chapter 5)
- Instructions for customizing NTP (Chapter 6)
- Descriptions of TCP, FTP, Telnet, and NTP parameters with instructions for editing (Appendix A)
- Default parameter settings (Appendix B)

Before You Begin

Before using this guide, you must complete the following procedures:

- Create and save a configuration file that has at least one IP interface.
- Retrieve the configuration file in local, remote, or dynamic mode.

Refer to *Configuring Routers* or *Configuring Customer Access and Trunks (BNX Software)*, depending on your platform, for instructions on how to perform these functions.

Conventions

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: if command syntax is **ping** *<ip_address>*, you enter **ping 192.32.10.12**
bold text	Indicates text that you need to enter, command names, and buttons in menu paths. Example: Enter **wfsm &**
	Example: Use the **dinfo** command.
	Example: ATM DXI > Interfaces > **PVCs** identifies the PVCs button in the window that appears when you select the Interfaces option from the ATM DXI menu.
brackets ([ ])	Indicate optional elements. You can choose none, one, or all of the options.
ellipsis points	Horizontal (. . .) and vertical ellipsis points indicate omitted information.
italic text	Indicates variable values in command syntax descriptions, new terms, file and directory names, and book titles.
quotation marks (“ ”)	Indicate the title of a chapter or section within a book.
`screen text`	Indicates data that appears on the screen. Example: `Set Bay Networks Trap Monitor Filters`

separator (>)	Separates menu and option names in instructions and internal pin-to-pin wire connections. Example: Protocols > AppleTalk identifies the AppleTalk option in the Protocols menu. Example: Pin 7 > 19 > 20
vertical line (|)	Indicates that you enter only one of the parts of the command. The vertical line separates choices. Do not type the vertical line when entering the command. Example: If the command syntax is **show at routes | nets**, you enter either **show at routes** or **show at nets**, but not both.

Acronyms

ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
BNX	Backbone Node Switch
CMIP	Common Management Information Protocol
DARPA	Defense Advanced Research Projects Agency (formerly ARPA)
DLSw	data link switching
EGP	Exterior Gateway Protocol
FDDI	Fiber Distributed Data Interface
FIFO	first in first out
FTP	File Transfer Protocol
GMT	Greenwich Mean Time
IEEE	Institute of Electrical and Electronic Engineers
ILI	Intelligent Link interface
IP	Internet Protocol
LAN	local area network
MIB	management information base
MAC	media access control
NTP	Network Time Protocol
MOP	Maintenance Operations Protocol

OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PVC	permanent virtual circuit
QENET	Quad Ethernet Link Module
RFC	Request for Comment
RIP	Routing Information Protocol
SMDS	Switched Multimegabit Data Services
SNAP	Subnetwork Access Protocol
SNMP	Simple Network Management Protocol
SRM	system resource module
SVC	switched virtual circuit
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol
WAN	wide area network

Ordering Bay Networks Publications

To purchase additional copies of this document or other Bay Networks publications, order by part number from the Bay Networks Press™ at the following telephone or fax numbers:

- Telephone - U.S./Canada 1-888-4BAYPRESS
- Telephone - International 1-510-490-4752
- Fax 1-510-498-2609

You can also use these numbers to request a free catalog of Bay Networks Press product publications.

Technical Support and Online Services

To ensure comprehensive network support to our customers and partners worldwide, Bay Networks Customer Service has Technical Response Centers in key locations around the globe:

- Billerica, Massachusetts
- Santa Clara, California
- Sydney, Australia
- Tokyo, Japan
- Valbonne, France

The Technical Response Centers are connected via a redundant Frame Relay Network to a Common Problem Resolution system, enabling them to transmit and share information, and to provide live, around-the-clock support 365 days a year.

Bay Networks Information Services complement the Bay Networks Service program portfolio by giving customers and partners access to the most current technical and support information through a choice of access/retrieval means. These include the World Wide Web, CompuServe, Support Source CD, Customer Support FTP, and InfoFACTS document fax service.

Bay Networks Customer Service

If you purchased your Bay Networks product from a distributor or authorized reseller, contact that distributor's or reseller's technical support staff for assistance with installation, configuration, troubleshooting, or integration issues.

Customers can also purchase direct support from Bay Networks through a variety of service programs. As part of our PhonePlus™ program, Bay Networks Service sets the industry standard, with 24-hour, 7-days-a-week telephone support available worldwide at no extra cost. Our complete range of contract and noncontract services also includes equipment staging and integration, installation support, on-site services, and replacement parts delivery -- within approximately 4 hours.

To purchase any of the Bay Networks support programs, or if you have questions on program features, use the following numbers:

Region	Telephone Number	Fax Number
United States and Canada	1-800-2LANWAN; enter Express Routing Code (ERC) 290 when prompted (508) 436-8880 (direct)	(508) 670-8766
Europe	(33) 92-968-300	(33) 92-968-301
Asia/Pacific Region	(612) 9927-8800	(612) 9927-8811
Latin America	(407) 997-1713	(407) 997-1714

In addition, you can receive information on support programs from your local Bay Networks field sales office, or purchase Bay Networks support directly from your authorized partner.

Bay Networks Information Services

Bay Networks Information Services provide up-to-date support information as a first-line resource for network administration, expansion, and maintenance. This information is available from a variety of sources.

World Wide Web

The Bay Networks Customer Support Web Server offers a diverse library of technical documents, software agents, and other important technical information to Bay Networks customers and partners.

A special benefit for contracted customers and resellers is the ability to access the Web Server to perform Case Management. This feature enables your support staff to interact directly with the network experts in our worldwide Technical Response Centers. A registered contact with a valid Site ID can

- View a listing of support cases and determine the current status of any open case. Case history data includes severity designation, and telephone, e-mail, or other logs associated with the case.
- Customize the listing of cases according to a variety of criteria, including date, severity, status, and case ID.
- Log notes to existing open cases.
- Create new cases for rapid, efficient handling of noncritical network situations.
- Communicate directly via e-mail with the specific technical resources assigned to your case.

The Bay Networks URL is *http://www.baynetworks.com*. Customer Service is a menu item on that home page.

Customer Service FTP

Accessible via URL *ftp://support.baynetworks.com* (134.177.3.26), this site combines and organizes support files and documentation from across the Bay Networks product suite, including switching products from our Centillion™ and Xylogics® business units. Central management and sponsorship of this FTP site lets you quickly locate information on any of your Bay Networks products.

Support Source CD

This CD-ROM -- sent quarterly to all contracted customers -- is a complete Bay Networks Service troubleshooting knowledge database with an intelligent text search engine.

The Support Source CD contains extracts from our problem-tracking database; information from the Bay Networks Forum on CompuServe; comprehensive technical documentation, such as Customer Support Bulletins, Release Notes, software patches and fixes; and complete information on all Bay Networks Service programs.

You can run a single version on Macintosh Windows 3.1, Windows 95, Windows NT, DOS, or UNIX computing platforms. A Web links feature enables you to go directly from the CD to various Bay Networks Web pages.

CompuServe

For assistance with noncritical network support issues, Bay Networks Information Services maintain an active forum on CompuServe, a global bulletin-board system. This forum provides file services, technology conferences, and a message section to get assistance from other users.

The message section is monitored by Bay Networks engineers, who provide assistance wherever possible. Customers and resellers holding Bay Networks service contracts also have access to special libraries for advanced levels of support documentation and software. To take advantage of CompuServe's recently enhanced menu options, the Bay Networks Forum has been re-engineered to allow links to our Web sites and FTP sites.

We recommend the use of CompuServe Information Manager software to access these Bay Networks Information Services resources. To open an account and receive a local dial-up number in the United States, call CompuServe at 1-800-524-3388. Outside of the United States, call 1-614-529-1349, or your nearest CompuServe office. Ask for Representative No. 591. When you're on line with your CompuServe account, you can reach us with the command **GO BAYNET**.

InfoFACTS

InfoFACTS is the Bay Networks free 24-hour fax-on-demand information service. This automated system has libraries of technical and product documents designed to help you manage and troubleshoot your Bay Networks products. The system responds to a fax from the caller or to a third party within minutes of being accessed.

To use InfoFACTS in the United States or Canada, call toll-free 1-800-786-3228. Outside of North America, toll calls can be made to 1-408-764-1002. In Europe, toll-free numbers are also available for contacting both InfoFACTS and CompuServe. Please check our Web page for the listing in your country.

How to Get Help

Use the following numbers to reach your Bay Networks Technical Response Center:

Technical Response Center	Telephone Number	Fax Number
Billerica, MA	1-800-2LANWAN	(508) 670-8765
Santa Clara, CA	1-800-2LANWAN	(408) 764-1188
Valbonne, France	(33) 92-968-968	(33) 92-966-998
Sydney, Australia	(612) 9927-8800	(612) 9927-8811
Tokyo, Japan	(81) 3-5402-0180	(81) 3-5402-0173

Chapter 1
Starting TCP, FTP, Telnet, and NTP

TCP, FTP, Telnet, and NTP are application protocols that support the Bay Networks implementation of IP.

You can easily start TCP, FTP, Telnet, and NTP and configure them on a circuit using the default parameter values that Site Manager supplies. After you have done that, you can customize the configuration any way you like. Chapter 2, "TCP, FTP, Telnet, and NTP Concepts," looks at how the protocols work. Chapters 3 through 6 describe how you configure these protocols by editing their default parameter values.

Preparing a Configuration File

After you start Site Manager, prepare a configuration file as follows:

1. **Select the Configuration Manager in either local, remote, or dynamic mode from the Tools menu.**
2. **Open the configuration file in local or remote mode.**
3. **Select the appropriate router type (for example, BLN®).**
4. **Specify the router hardware (if you are using a local mode configuration file).**

   Specify an empty slot and select the link or net module connector you want to insert in the slot.

Configuring IP on a Circuit

Before you can select TCP, FTP, Telnet, and NTP to run on the router, you must configure a circuit and add the IP protocol to it, using the default values. IP uses this circuit as an interface to the attached network. For instructions on adding IP to a circuit, refer to *Configuring IP Services*.

With these tasks completed, you have a fully operational IP connection configured with the default values.

Starting TCP

This section describes how to get TCP started on a circuit and how to create and delete TCP on a router. It assumes you have read *Configuring Routers.*

Creating TCP on a Router

To enable TCP on your router after you have configured IP on a circuit, you can configure TCP services globally on the same circuit.

You configure TCP services globally using Site Manager.

Site Manager Path: From the Configuration Manager window, select Protocols > Global Protocols > TCP > Create TCP. The Edit TCP Global Parameters window opens, allowing you to edit the TCP global parameters.

Deleting TCP from the Router

Caution: The system automatically deletes Telnet from the router when you delete TCP.

You can use Site Manager to delete TCP on your router.

Site Manager Path: From the Configuration Manager window, select Protocols > Global Protocols > TCP > Delete TCP. Click on OK in the Confirmation window. Site Manager deletes TCP from the router.

Customizing TCP

For information on modifying TCP default parameters to customize the way TCP runs on your router, see Chapter 3.

Starting FTP

This section describes how to get an FTP server running on a circuit and how to create and delete an FTP server on a router. It assumes you have read *Configuring Routers.*

Creating an FTP Server on the Router

Before you can create an FTP server on your router, you must first configure TCP and IP on a circuit. For instructions on how to configure IP, see "Configuring IP on a Circuit." For instructions on how to configure TCP, see "Starting TCP."

You can create an FTP server using Site Manager.

Site Manager Path: From the Configuration Manager window, select Protocols > Global Protocols > FTP > Create FTP. Site Manager creates FTP on the router.

Deleting an FTP Server from the Router

You can delete an FTP server from the router using Site Manager.

Site Manager Path: From the Configuration Manager window, select Protocols > Global Protocols > FTP > Delete FTP. Site Manager asks: `Do you really want to delete FTP?` Click on OK to delete FTP from the router.

Customizing FTP

For information on modifying FTP default parameters to customize the way FTP runs on your router, see Chapter 4.

Starting Telnet

This section describes how to get Telnet Client and Telnet Server running on a circuit and how to create and delete Telnet on a router. It assumes you have read *Configuring Routers.*

Creating Telnet on the Router

Before you can create Telnet on the router, you must first configure TCP IP on a circuit. For instructions on how to configure IP, see “Configuring IP on a Circuit.” For instructions on how to configure TCP, see “Starting TCP.”

You can create a Telnet Client or Telnet Server using Site Manager.

Site Manager Path: From the Configuration Manager window, select Protocols > Global Protocols >Telnet Client | Telnet Server > Create Telnet Client | Telnet Server. For Telnet Server, the Telnet Configuration window opens, allowing you to edit Telnet Server global parameters.

Deleting Telnet from the Router

You can use Site Manager to delete Telnet Client or Telnet Server from the router.

Site Manager Path: From the Configuration Manager window, select Protocols > Global Protocols > Telnet Client | Telnet Server > Delete Telnet Client | Telnet Server. Site Manager asks: `Do you really want to delete Telnet Client | Server?` Click on OK to delete Telnet from the router.

Customizing Telnet

You can customize the way that Telnet Client and Telnet Server run on your router by modifying the default Telnet parameter values. For more information, see Chapter 5.

Starting NTP

This section describes how to get NTP started on a circuit and how to create and delete NTP on a router. It assumes you have read *Configuring Routers.*

Creating NTP on the Router

Before you can create NTP on the router, you must first configure IP on the router. For instructions on how to configure IP, see “Configuring IP on a Circuit.”

When you configure IP, you should select a routing protocol, such as RIP or OSPF, if you have configured remote time servers on your network. NTP requires a routing protocol to synchronize the remote time servers with primary time servers. For instructions on how to configure RIP, refer to *Configuring IP Services*.

You can create NTP on the router using Site Manager.

Site Manager Path: From the Configuration Manager window, select Protocols > Global Protocols > NTP > Create NTP.

Deleting NTP from the Router

You can use Site Manager to delete NTP from the router.

Site Manager Path: From the Configuration Manager window, select Protocols > Global Protocols > NTP > Delete NTP. Click on OK in the confirmation window to delete NTP from the router.

Customizing NTP

You can customize the way NTP runs on your router by modifying its default parameter values. For information on modifying default NTP default parameter values, see Chapter 6.

Where to Go Next

The following table shows you where to find additional information for configuring and customizing TCP, FTP, Telnet, and NTP.

For information on	Go to
TCP, Telnet, FTP, and NTP and how Bay Networks implements these protocols	Chapter 2
How to configure TCP services	Chapter 3
How to configure FTP services	Chapter 4
How to configure Telnet services	Chapter 5
How to configure NTP services	Chapter 6
TCP, FTP, Telnet, and NTP parameter descriptions	Appendix A
TCP, FTP, Telnet, and NTP parameter default values	Appendix B

Chapter 2
TCP, FTP, Telnet, and NTP Concepts

This chapter describes the concepts behind TCP, FTP, Telnet, and NTP and how we implement them in Bay Networks routers. You can use this information to decide how to customize TCP, FTP, Telnet, and NTP parameters for your system.

TCP Overview

In the 1970s, the Defense Advanced Research Projects Agency (DARPA) of the U.S. Department of Defense (DOD) developed the Transmission Control Protocol (TCP) to provide communication among hosts manufactured by different vendors. DARPA designed TCP to work within a layered hierarchy of networking protocols, using the Internet Protocol (IP) to transfer data.

Built upon the IP layer suite, TCP is a connection-oriented, end-to-end protocol that provides the packet sequencing, error control, and other services required to provide reliable end-to-end communications. IP takes the packet from TCP and passes it along whatever gateways are needed, for delivery to the remote TCP layer through the remote IP layer.

The Bay Networks implementation of TCP generally ensures good terminal server performance on slow-speed links as well as high-speed LAN links. TCP Services are required to support upper-layer protocols, such as Telnet and FTP, which are part of the TCP/IP suite.

TCP does not require reliability of the communication protocols below itself. Therefore, TCP functions with lower-level protocols that are simple, potentially unreliable datagram services. TCP uses IP for a lower-level protocol.

How TCP Works

TCP is connection-oriented. Therefore, before transferring data, you must first establish a logical transport layer connection with a peer user. To establish this connection, TCP uses what is sometimes called a “three-way handshake,” in which the initiating TCP sends a Protocol Data Unit (PDU) with a synchronize (SYN) bit set to 1 in its header. The responding TCP then sends back a PDU with both the SYN bit and the Acknowledge (ACK) bit set, and possibly, some user data. Time and, if necessary, retransmission are used to recover from PDUs lost in this process, allowing each side to indicate its starting sequence number. Because of the possibility of lost or delayed PDUs, this three-way exchange ensures that connections are established correctly.

Data transfer is straightforward, and follows the procedures for flow control and acknowledgment. TCP performs all acknowledgment and assigns all credits in terms of octets. A credit of eight (8), then, allows sending only 8 octets of data, not 8 PDUs.

To release a connection, one TCP sends a PDU with the FIN flag set and a sequence number one greater than that assigned to the last octet of the transmitted data. Upon receipt of this PDU, the responding TCP sends back a PDU carrying an ACK for the FIN’s sequence number and a FIN of its own (this ACK or FIN may appear in the same PDU or in different PDUs). The TCP that sent the first FIN must respond with an ACK for this new FIN. This rather complex procedure allows a graceful close, ensuring that no data is lost during release of the connection.

TCP Features

Since IP does not always guarantee reliable transfer of data, TCP implements several reliability features to ensure that data arrives at its destination uncorrupted and in the order sent. Table 2-1 describes these features.

Table 2-1. TCP Reliability Features

Feature	Description
Sequence numbers	TCP assigns a sequence number to each data segment it transmits. The receiving host uses the sequence numbers to make sure that all the data arrives in order. TCP assigns sequence numbers on a per-octet basis, so the value in this field is actually the sequence number of the first octet of the user data.
Out-of-order caching	As TCP receives data segments, it puts them in sequential order and forwards them to the receiving TCP client. If TCP fails to receive one or more segments and cannot complete the sequential ordering, it stores the remaining segments in cache memory for as long as the TCP connection exists. When TCP receives the missing segments, it takes the stored segments from cache memory, puts them into sequential order with the newly received segments, and then forwards them to the receiving TCP client. Out-of-order caching ensures that data arrives in the correct order while saving bandwidth and retransmission time.
Checksums	To ensure the integrity of the data, the sending host adds a checksum to each segment it transmits. The receiving host recalculates the checksum, and if there is damage, discards the segment.
Flow control	Flow control allows the receiving host to regulate how much data is sent to it. To activate flow control, the receiving host advertises a *window* that indicates how much data it can accept. When the transmit window is full, the sending host must stop sending data until the receiving host can open the window again. To control the rate of data transfer on your TCP connections, you can specify the maximum window size allowed for each connection.
Acknowledgment with retransmission	TCP requires the receiving host to acknowledge that it has received the data. If the sending host does not receive an acknowledgment within a set timeout interval, the sending station retransmits the data. TCP determines the timeout interval by estimating the average time it takes to send a segment and receive an acknowledgment for it.

Connection Types

TCP is a connection-oriented protocol that requires that application programs at both ends of the connection agree that a connection is desired before TCP traffic can pass across an internet. To do so, the application program at one end performs a passive open while the application program at the other end performs an active open. For passive opens, a TCP client (the process or application program that uses TCP) waits to accept incoming connection requests. Clients using passive opens can listen for specific connection requests or for a range of inbound requests. In an active open, the client initiates the connection. Once a connection has been created, application programs can begin to pass data; that is, the programs at each end exchange messages that guarantee reliable delivery.

Connections and Connection States

TCP establishes a set of access points, referred to as *ports*, for each host. It associates each port with a network and host address to form a *socket*. A pair of sockets, together with sequence numbers, window sizes, and status information, form a *TCP connection*.

Table 2-2 lists the states through which a TCP connection proceeds during its lifetime.

Table 2-2. TCP Connection States

State	Definition
LISTEN (2)	TCP listens for a connection request from any remote TCP.
SYN SENT (3)	TCP sent a connection request (SYN segment) and waits for a matching connection request and acknowledgment from the remote TCP.
SYNRECEIVED (4)	TCP sent a connection request, received a matching request, and waits for a confirming connection request acknowledgment from the remote TCP.
ESTABLISHED (5)	Connection open. Data can be received and sent. This is the normal state for the data transfer phase of the connection.
FINWAIT-1 (6)	TCP waits for a connection termination request (FIN segment) from the remote TCP, or for an acknowledgment of a previously sent connection termination request.

(continued)

Table 2-2. TCP Connection States *(continued)*

State	Definition
FINWAIT-2 (7)	TCP waits for a connection termination request from the remote TCP.
CLOSEWAIT (8)	TCP waits for a connection termination request from the client.
CLOSING (10)	TCP waits for a connection termination request acknowledgment from the remote TCP.
LASTACK (9)	TCP waits for acknowledgment of the connection termination request previously sent to the remote TCP.
TIMEWAIT (11)	TCP waits for enough time to pass to ensure that the remote TCP received the acknowledgment of its connection termination request.
CLOSED (1)	No connection.

TCP Memory Considerations

The Transmission Control Protocol requires a significant amount of memory to

- Retain copies of outbound data in case they must be retransmitted
- Retain copies of inbound data in case they are received out of order and must be rearranged
- Manage the TCP connections

The amount of memory used per TCP connection is dynamic. Each connection uses a small amount of overhead memory (less than 1 KB), even if the connection is idle. As the size of the transmit-and-receive window increases, so does the memory for connections. It expands as much as TCP allows.

You can control the window size by setting a value for the Max. Window Size parameter in the Edit TCP Global Parameters window (see Chapter 3). The maximum amount of memory TCP can use for a connection is equal to the overhead memory plus twice the window size (because the window can fill in both directions).

The value you set for Maximum Window Size depends on how much memory you need for services other than TCP. If you have a complicated configuration, specify a low Max. Window Size value for TCP connections, since space is limited. Systems with less involved configurations can support more TCP connections and a higher Maximum Window Size value.

If TCP consumes too much memory on the router, connections slow down or even abort. TCP uses feedback mechanisms to indicate to clients when resources are becoming scarce. However, if clients disregard this feedback, TCP has to break connections. TCP attempts to monitor the connections consuming the most memory and break those first to maintain connections consuming less memory.

TCP and IP Service Users

TCP is the layer or service between IP, at the lower layer in the hierarchy of network protocols, and programs running at higher layers in the hierarchy. Figure 2-1 shows a simple network architecture with four users of TCP/IP services: data link switching (DLSw), Telnet, FTP, and BGP.

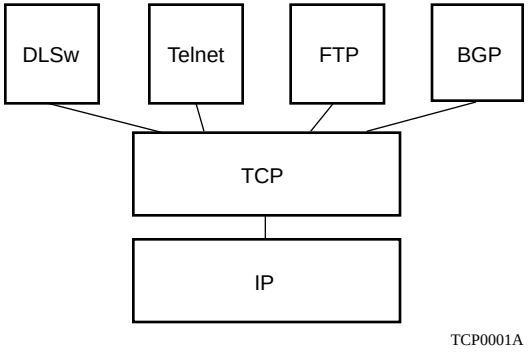

Figure 2-1. TCP between IP and Clients

The interface between TCP and programs that use TCP consists of a set of messages exchanged between the clients and TCP, and a set of functions and macros that user programs call to exchange TCP messages. These programs use the functions and macros to

- Open, close, abort, and get the status of connections
- Control the flow of data
- Encapsulate data for TCP to transmit
- Process received TCP data

When a program passes data to TCP, the TCP layer formats the data and calls on the IP layer to transmit the data to its destination.

For information on creating TCP on the router, see Chapter 1. For information on editing TCP parameters, see Chapter 3.

FTP Overview

The File Transfer Protocol allows files to be transferred from a server to an FTP client or from an FTP client to the server. FTP ensures the integrity of data transferred from one system to another.

Using FTP, you can log in to a remote host, identify yourself, list remote directories, copy files to or from the remote host, and execute a few simple commands remotely.

When you enable FTP on the router, you can:

- Download files from a host system to a remote router and retrieve files from the router
- Examine the directory listing of files on the remote router
- Delete files on the remote router

As network administrator, you use Site Manager to create the FTP server on the router and edit FTP server parameters. For complete information and instructions, refer to Chapter 4.

How FTP Works

The FTP client initiates an FTP session with the FTP server on the router. The session establishes two separate connections between host and router as follows:

- Control connection -- the communication path between the FTP client and the FTP control server for the exchange of commands and replies used for sending a command request or response
- Data connection -- a full-duplex connection over which data is transferred in a specified mode and type between FTP client and FTP server

The FTP client residing on the host and the FTP server residing on the router rely on the underlying support of TCP and IP for the reliable, sequenced transfer of data and control messages (Figure 2-2).

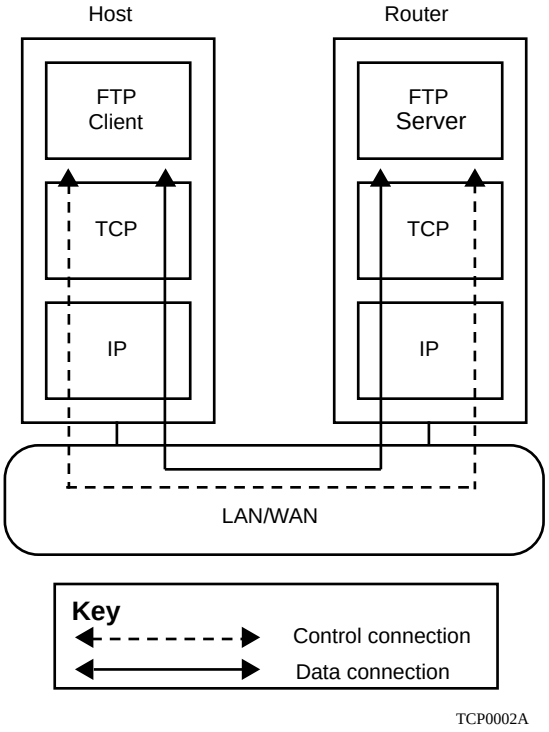

Figure 2-2. FTP Client and Server

Table 2-3 describes the FTP commands that the FTP server supports on Bay Networks routers.

Table 2-3. FTP Commands Supported

Command	Code	Description
Access Control Commands		
User Name	USER	Initiates an FTP session for the user.
Password	PASS	Specifies a user's encrypted identification for access control.
Logout	QUIT	Terminates the session and closes the control connection.
Transfer Parameter Commands		
Data Port	PORT	Specifies the data port to be used in the data connection.
Representation Type	TYPE	Specifies the data transfer type. The server supports transfer of ASCII and image (binary) data.
Transfer Mode	MODE	Specifies the transfer mode. The server supports stream mode only.
File Structure	STRU	Specifies the file structure type. The server supports file (no record) structure only.
FTP Service Commands		
Retrieve	RETR	Causes the server to transfer the specified file to the client.
Abort	ABOR	Causes the server to abort the previous FTP service command and any associated transfer of data.
Store	STOR	Causes the server to accept the data transferred over the data connection and store it on the server.
Store Unique	STOU	Specifies the same operation as the **Store** command and, in addition, causes the server to create the resulting file in the current directory under a name unique to that directory.
Delete	DELE	Causes the server to delete the specified file on the server.
List	LIST	Causes the server to send to the client a detailed list of files.
Name List	NLST	Causes the server to send to the client a list of filenames.
Status	STAT	Causes the server to send to the client the control connection status. If the server receives the command during file transfer, the server sends the client the status of the transfer.
Help	HELP	Provides helpful information.
No Operation	NOOP	Specifies no action. Causes the server to send an OK reply.

(continued)

Table 2-3. FTP Commands Supported *(continued)*

Command	Code	Description
Change Working Directory	CWD	Causes the server to change the volume.
Print Working Directory	PWD	Causes the server to print its current working directory.
Implementation-specific FTP Commands		
Compact	COMP	Causes the server to compact the Flash card. Use this command after the **delete** command, or when the amount of contiguous space is low. You can determine the amount of contiguous space on a router by using the **dir** command.

Telnet Overview

Telnet is a virtual terminal protocol that is part of the TCP/IP protocol suite. It allows you to access any system on your network running the Telnet server software. Accessing Telnet establishes a virtual connection between your terminal and the specified host. Once you connect to a host through Telnet, your terminal appears to be connected directly to that host.

Telnet offers three basic services:

- It defines a network virtual terminal that provides a standard interface to remote systems. Clients do not have to understand the details of all possible remote systems; they are built to use the standard interface.
- It allows client and server to negotiate options, and it provides a set of standard options.
- It treats both ends of the connection symmetrically. So, instead of forcing the client side to connect to a user's terminal, Telnet allows an arbitrary program to become a client. Furthermore, either end of the connection can negotiate options.

Telnet is used primarily to access the Technician Interface. You can execute Technician Interface commands from a remote host (inbound Telnet) or originate an outgoing Telnet session (outbound Telnet) to another Bay Networks router or network device that accepts Telnet. You use outbound Telnet to access remote routers when Site Manager or Simple Network Management Protocol (SNMP) is unavailable.

To use Telnet to access the Technician Interface, you must assign at least one IP address to the router. The number of Telnet connections you can make to the Technician Interface is limited only by the availability of system resources (that is, system memory).

Note: We recommend that you establish no more than one Telnet session per router.

How Telnet Works

Before you can enable Telnet on the router, you must first create TCP. After you create TCP, you can create Telnet Server and Telnet Client and modify their default parameters. For information on creating TCP and modifying Telnet default parameters, see Chapter 5.

Telnet Server

When you create a Telnet server, the router accepts inbound requests from a Telnet client and establishes a Telnet session to the Technician Interface.

A PC with a network configuration can run a Telnet terminal emulation program to establish a remote session on a router (Figure 2-3). In this case, the PC is defined as a Telnet client and the router as a Telnet server.

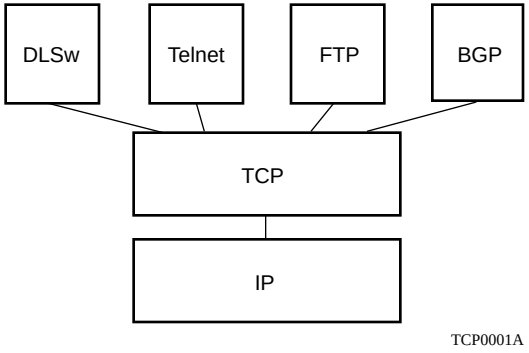

Figure 2-3. Telnet Server

Telnet Client

When you create a Telnet client, the router sends outbound requests to a remote host to establish a Telnet session on a remote node. Once the router establishes the Telnet session, you can access all Technician Interface commands.

If you had established a terminal/console cable connection to a router, you could log in to the local router and use the Telnet command to establish a remote session on a remote router (Figure 2-4). In this case, the local router is defined as the Telnet client and the remote router as the Telnet server.

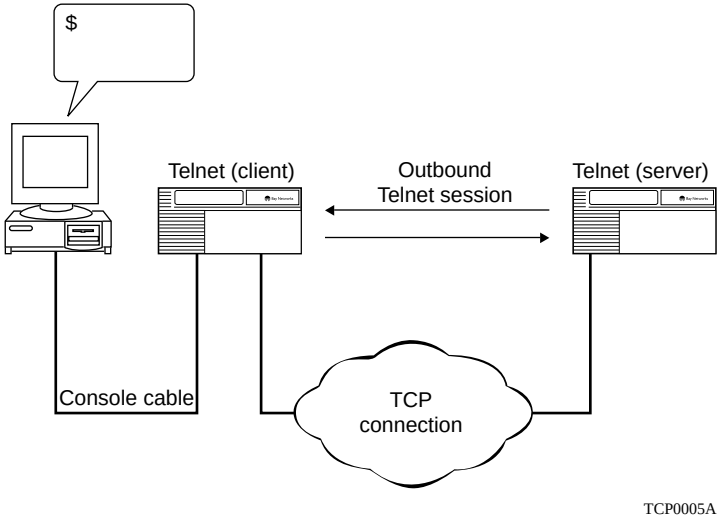

Figure 2-4. Telnet Client

For information on creating Telnet on the router and editing Telnet parameters, refer to Chapter 5.

NTP Overview

The Network Time Protocol (NTP) synchronizes the timing of internal clocks of various internet devices across large, diverse networks. NTP runs over UDP, which in turn runs over IP. The NTP protocol specification is documented in RFC 1305.

Each router on the network contains an internal system clock that is used to maintain accurate time for the router. NTP adjusts each clock's time to universal standard time. Because NTP is unaware of the Greenwich mean time (GMT) time zones, you need to set the time zones using the **date** command from the Technician Interface.

NTP Architecture

The NTP architecture model is based on a hierarchy consisting of an NTP client and primary and secondary time servers. The NTP client is an internet device that receives time information from an NTP time server and synchronizes its internal clock to it. The NTP client does not forward time information to other internet devices running NTP.

A primary time server is the authoritative time source in the hierarchy, meaning that it is the one true time source to which the other NTP devices will synchronize their internal clocks. Located at the root of the hierarchy, the primary time server is synchronized by a wire or radio clock to universal standard time. Secondary time servers synchronize with primary time servers or other secondary time servers to form a synchronization subnet (Figure 2-5.) Secondary time servers are located at successive levels from the primary time server based on timer accuracy and stratum level.

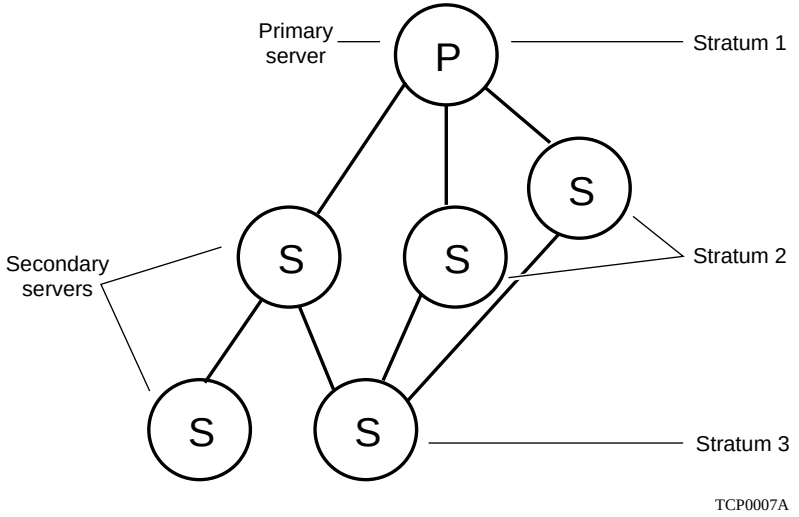

Figure 2-5. Time Servers Forming a Synchronization Subnet

Distributing Time Throughout the NTP Network

Time is distributed through a hierarchy of NTP servers, with each server adopting a “stratum,” which defines how many NTP “hops” away a particular secondary time server is from a primary time server on the network. A “stratum 1” time server has a wire or radio clock directly attached and is located at the top of the hierarchy (or bottom, depending on your point of view); a “stratum 2” time server receives its time via NTP from a “stratum 1” time server; a “stratum 3” time server receives its time via NTP from a “stratum 2” time server; and so forth. A time server running NTP automatically chooses as its time source the server with the lowest stratum number that it is configured to communicate with via NTP. This strategy effectively builds a self-organizing tree of NTP speakers. The number of strata is limited to 15 to avoid long-lived synchronization loops.

NTP tries not to synchronize to a server whose time might not be accurate. It avoids doing this in two ways. First, NTP never synchronizes to a time server that is not in turn synchronized itself. Second, NTP compares the time reported by several servers, and will not synchronize to a server whose time is markedly different from the others, even if its stratum is lower.

Synchronizing with the Best Available Time Server

Each NTP client in the synchronization subnet chooses the best available time server from which to synchronize its internal clock. NTP uses the following criteria to determine the time server whose time is best:

- Time server with the lowest stratum
- Time server closest in proximity to the primary time server (reduces network delays)
- Time server offering the highest claimed precision

NTP prefers to have access to several (at least three) servers at the lower stratum level, since it can apply an agreement algorithm to detect a problem on any part of the time source.

NTP Client Modes

NTP provides three modes (or associations) in which servers and clients can communicate with each other: Unicast Client mode, Broadcast Client mode, and Multicast Client mode. Currently, Bay Networks supports only NTP Client mode.

NTP servers and clients form an NTP relationship and maintain an association instance when they exchange messages.

Unicast Client Mode

You use Unicast Client mode primarily to configure a set of time servers (or peers) for time synchronization. You can also configure access control filters for time servers in Unicast Client mode, but normally you would perform this operation in Broadcast Client or Multicast Client mode. For more information on performing these tasks, see Chapter 6.

When you configure a set of time servers (peers) in Unicast Client mode, NTP creates a peer list that includes each time server's IP address. The NTP client uses the peer list to determine which time servers to query for time information. When the NTP client queries the time servers from the peer list, the time servers respond with various time stamps, along with information about their clocks, such as stratum, precision, and time reference (Figure 2-6). The NTP client reviews a list of responses from all the available servers and chooses one server as the "best" available time source from which to synchronize its internal clock.

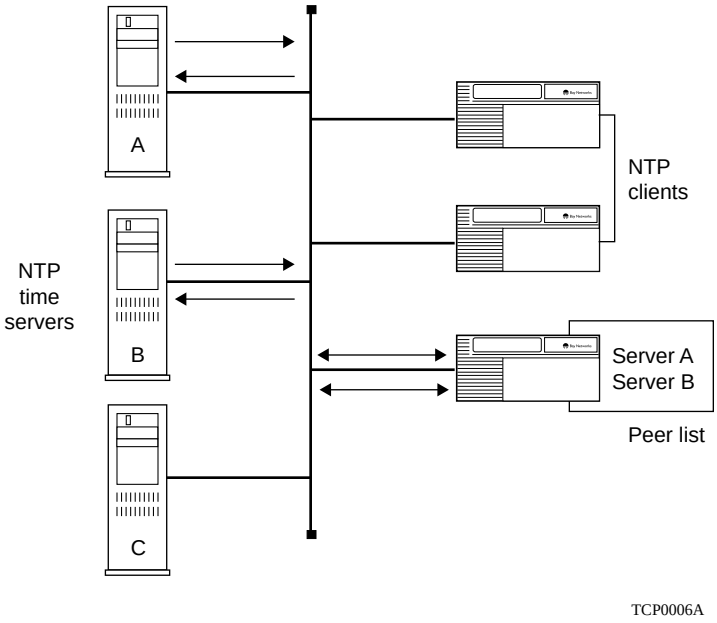

Figure 2-6. NTP Time Servers Operating in Unicast Client Mode

Broadcast and Multicast Client Mode

In Broadcast Client and Multicast Client modes, the NTP client receives NTP packets from every time server on the network, provided the IP address of the NTP packet matches the IP broadcast address of the NTP client. Once the NTP client receives NTP packets, it applies rules based on the NTP protocol to select the time server with the greatest accuracy.

In Broadcast Client and Multicast Client modes, you can restrict specific time servers from sending NTP packets to an NTP client by configuring access control filters. You cannot, however, configure peers in either Broadcast Client or Multicast Client mode.

Broadcast Client mode and Multicast Client mode are useful when you have many clients on the network and only one server, as broadcasting reduces overall traffic volume on the network.

Where to Go Next

The following table shows you where to find additional information for configuring and customizing TCP, FTP, Telnet, and NTP.

For information on	Go to
How to configure TCP services	Chapter 3
How to configure FTP services	Chapter 4
How to configure Telnet services	Chapter 5
How to configure NTP services	Chapter 6
TCP, FTP, Telnet, and NTP parameter descriptions	Appendix A
TCP, FTP, Telnet, and NTP parameter default values	Appendix B

Chapter 3
Customizing TCP Services

This chapter describes how to create and customize TCP services on the router. It assumes you have configured TCP on the interface using the default parameters, as described in Chapter 1, and that you understand the TCP concepts described in Chapter 2. You should have read *Configuring Routers* or *Configuring Customer Access and Trunks (BNX Software)*, as appropriate for your platform, and have performed the following tasks:

1. **Opened a configuration file in local or remote mode**
2. **Selected the appropriate router type, specified a slot, and selected the link or net module you want to insert in the slot (if you are using a local mode configuration file)**
3. **Configured IP on an interface using the default parameters, as described in Chapter 1**
4. **Created TCP in the Configuration Manager window**

TCP is a global parameter. You can create and enable TCP easily by using all the default parameter values that the Configuration Manager supplies.

If you decide to change some or all of the default parameters, refer to the instructions in this chapter. For a list of the TCP parameters, see Appendix B.

Configuring TCP on the Router

The following sections describe information you supply and options you select that affect the way TCP runs on the router.

Enabling and Disabling TCP

After you create TCP on the router, as described in Chapter 1, TCP is enabled on the IP circuit that you configured, and the default values are in effect for all TCP parameters (see parameter descriptions in Appendix A). You may want to change these values, depending on the requirements of your network.

If you want to disable TCP, select Disable. Also, you can select Disable if you do not need TCP, but want to access previous TCP statistics. Disable TCP is a global function. When you disable TCP, it is no longer available on all IP circuits.

Site Manager: Enable/Disable parameter: page A-2

Setting Minimum Retransmission Timeout

You can specify a minimum value for the retransmission timeout. When one side of a TCP connection sends a frame and does not receive an acknowledgment from the other side of the connection within the timeout period, the sending station retransmits the frame.

If you are transmitting on a high-speed network and you set the minimum retransmission timeout value too high, network performance may degrade because TCP must wait for the timeout period to elapse before retransmitting unacknowledged data.

Site Manager: Min. Retransmission Timeout (msec.) parameter: page A-2

Setting Maximum Retransmission

You can specify a maximum value for the retransmission timeout. When one side of a TCP connection sends a frame and does not receive an acknowledgment from the other side of the connection within the timeout period, the sending station retransmits the frame.

If you are transmitting on a low-speed network and you set the maximum retransmission timeout value too low, the network may become congested as TCP retransmits unacknowledged frames that have not yet reached their destination.

Setting Maximum Window Size (bytes)

Site Manager: Max. Retransmission Timeout (msec.) parameter: page A-3

You can specify a value in bytes to determine the maximum transmit-and-receive window size that TCP allows for each connection. The larger the window size, the more memory each TCP connection consumes.

Site Manager: Max. Window Size (bytes) parameter: page A-3

For More Information about TCP

If you would like more information about the Transmission Control Protocol, refer to

Comer, Douglas E. *Internetworking with TCP/IP, Volume I: Principles, Protocols, and Architecture*. Englewood Cliffs, New Jersey: Prentice Hall, Inc., Second Edition, 1991.

Where to Go Next

The following table shows you where to find additional information for configuring and customizing TCP, FTP, Telnet, and NTP.

For information on	Go to
TCP, Telnet, FTP, and NTP and how Bay Networks implements these protocols	Chapter 2
How to configure FTP services	Chapter 4
How to configure Telnet services	Chapter 5
How to configure NTP services	Chapter 6
TCP, FTP, Telnet, and NTP parameter descriptions	Appendix A
TCP, FTP, Telnet, and NTP parameter default values	Appendix B

Chapter 4
Customizing FTP Services

This chapter describes how to create and customize FTP services on the router. You should have read *Configuring Routers* or *Configuring Customer Access and Trunks (BNX Software)*, as appropriate for your platform, and have performed the following tasks:

1. **Opened a configuration file in local or remote mode**
2. **Selected the appropriate router type, specified a slot, and selected the link or net module you want to insert in the slot (if you are using a local mode configuration file)**
3. **Configured IP on an interface using the default parameters, as described in Chapter 1**
4. **Created TCP in the Configuration Manager window**
5. **Created FTP in the Configuration Manager window**

You can create and enable FTP easily by using all the default parameter values that the Configuration Manager supplies.

If you decide to change some or all of the default parameters, refer to the instructions in this chapter. For a list of FTP parameters, see Appendix B.

Configuring the FTP Server on the Router

The following section describes information you supply and options you select that affect the way the FTP server runs on the router.

Enabling and Disabling an FTP Server

After you create FTP on the router, as described in Chapter 1, default values are in effect for all FTP parameters (see parameter descriptions in Appendix A). You may want to change these parameter values, depending on the requirements of your network.

Site Manager: Enable/Disable parameter: page A-4

Specifying the FTP Default Volume

The FTP default volume is the file system volume to which FTP writes transferred files and from which FTP retrieves files for transfer. To specify the FTP default volume, you must specify a value between 1 and 13 for the file system volume. On diskette-based systems, you must specify Volume A as the default volume.

Site Manager: Default Volume parameter: page A-4

Specifying Login Retries Value

The FTP login retries value is the number of FTP login retries that FTP will accept before rejecting logins. By default, FTP accepts only three FTP login retries before rejecting subsequent logins.

Site Manager: Login Retries parameter: page A-4

Specifying Maximum FTP Idle Time

The FTP idle time is the length of time (in seconds) that FTP waits before closing an idle FTP control connection. You must determine the maximum idle time you want to allow and specify the time value in seconds. By default, FTP waits 900 seconds before closing an idle FTP control connection.

Site Manager: Idle Time Out (secs) parameter: page A-5

Specifying Maximum FTP Sessions

You can determine the maximum number of FTP sessions you want to run simultaneously by specifying a value. Determine the maximum number of simultaneous sessions you want to allow and specify a value from 1 through 10000.

By default, FTP allows you to run a maximum of three FTP sessions.

Site Manager: Max. Sessions parameter: page A-5

Specifying the Data Transmission Type

You can select the data transmission type by specifying either ASCII characters or binary.

Site Manager: Type of Service parameter: page A-5

Specifying the FTP Control Connection

You can determine how the Internet transport layer handles datagrams on a control data connection by specifying the Type of Service value that FTP inserts in IP datagrams on a control connection.

Site Manager: Control Connection parameter: page A-6

Specifying a Data Transfer Value

You can determine how the Internet transport layer handles datagrams on a data transfer connection by specifying a value that indicates the Type of Service that FTP inserts in IP datagrams on a data transfer connection.

Site Manager: Data Transfer parameter: page A-6

Specifying the TCP Window Size

You can determine the size of the window you want to use for TCP connections by specifying its size in bytes.

Site Manager: TCP Window Size parameter: page A-6

Where to Go Next

The following table shows you where to find additional information for configuring and customizing TCP, FTP, Telnet, and NTP.

For information on	Go to
TCP, FTP, Telnet, and NTP and how Bay Networks implements these protocols	Chapter 2
How to configure TCP services	Chapter 3
How to configure Telnet services	Chapter 5
How to configure NTP services	Chapter 6
TCP, FTP, Telnet, and NTP parameter descriptions	Appendix A
TCP, FTP, Telnet, and NTP parameter default values	Appendix B

Chapter 5
Customizing Telnet Services

This chapter describes how to create and customize Telnet Server and Telnet Client on the router. You should have read *Configuring Routers* or *Configuring Customer Access and Trunks (BNX Software)*, as appropriate for your platform, and have performed the following tasks:

1. **Opened a configuration file in local or remote mode**
2. **Selected the appropriate router type, specified a slot, and selected the link or net module that you want to insert in the slot (if you are using a local mode configuration file)**
3. **Configured IP on an interface using the default parameters, as described in Chapter 1**
4. **Created TCP in the Configuration Manager window**
5. **Created Telnet Client or Telnet Server in the Configuration Manager window**

You can create and enable Telnet services easily by using all the default parameter values that the Configuration Manager supplies.

If you decide to change some or all of the default parameters, refer to the instructions in this chapter. For a list of Telnet parameters, see Appendix B.

Configuring a Telnet Server on the Router

After you create a Telnet Server on the router for inbound Telnet sessions, as described in Chapter 2, default values are in effect for all Telnet Server parameters (see parameter descriptions in Appendix A). You may want to change these parameter values, depending on the requirements of your network.

The following sections describe information you supply and options you select that affect the way Telnet Server runs on the router.

Changing the Login Script Information

The script files for the Manager's Login, User's Login, and Force User Logout run automatically when you log in. You can accept the defaults, or customize the scripts as needed.

Changing the Name of the Manager's Login Script File

By default, the name of the Manager's script file is *automgr.bat*. You can specify a new name for the Manager's Login script by supplying an 8-character filename. If you do not want to change the name of the Manager's Login script, accept the default name.

Site Manager: Manager's Login Script parameter: page A-12

Changing the Name of the User's Login Script File

By default, the name of the User's Login script file is *autouser.bat*. You can specify a new name for the User's Login script file by supplying an 8-character filename. If you do not want to change the name of the User's Login script, accept the default name.

Site Manager: User's Login Script parameter: page A-7

Enabling and Disabling User Logout

By default, you can press control-c to cancel the user autoscript at login and access the Technician Interface. When you select Enable, you cannot use control-c to cancel the user autoscript at login (when a user autoscript is in effect).

Site Manager: Force User Logout parameter: page A-7

Changing the Telnet Configuration on the Router

This section describes how to customize your Telnet session on the router.

Enabling and Disabling Telnet for the IP Router

You can enable or disable Telnet for the IP router. By default, Telnet is enabled for the IP router, allowing you to establish Telnet sessions to the Technician Interface. Select Disable to disable Telnet for the IP router.

Site Manager: Enable/Disable parameter: page A-8

Specifying the Maximum Number of Lines on the Technician Interface Console

You can specify the maximum number of lines displayed on the Telnet Technician Interface console screen. The screen may override the number of lines you specify if Telnet can negotiate the window size with the remote client. By default, the maximum number of lines displayed on the Telnet Technician Interface console screen is 24.

Site Manager: TI Lines per Screen parameter: page A-8

Using the Pause Feature

By default, the Technician Interface pauses after each screen fills with data. You can configure the Technician Interface not to pause after each screen fills with data by disabling this feature.

Site Manager: TI More parameter: page A-9

Changing the Telnet Login Prompt

You can change the Telnet login prompt on the Telnet console screen by specifying a character string from 1 through 18 alphanumeric characters.

Site Manager: TI Prompt parameter: page A-9

Changing the Login Timeout

You can specify a value that will determine the number of minutes that can elapse before the Technician Interface disconnects the Telnet session if you fail to enter a login ID at the login prompt. By default, the Technician Interface waits 1 minute before it disconnects the Telnet session if you fail to enter a login ID at the login prompt.

Site Manager: Login Timeout (min.) parameter: page A-9

Changing the Password Timeout

By changing the password timeout value you can determine the number of minutes that can elapse before the Technician Interface disconnects the Telnet session if you do not enter a password at the password prompt. By default, the Technician Interface waits 1 minute before it disconnects the Telnet session if you fail to enter a password at the password prompt.

Site Manager: Password Timeout (min.) parameter: page A-10

Changing the Command Timeout

By changing the command timeout you determine the number of minutes that can elapse before the Technician Interface disconnects the Telnet session if you do not enter a command at the command prompt. The default value is 15 minutes.

Site Manager: Command Timeout (min.) parameter: page A-10

Changing Login Retries

By changing the login retries you can determine the maximum number of login attempts you can make before the Technician Interface disconnects the Telnet session. The default value is three login attempts.

Site Manager: Login Retries parameter: page A-10

Using Telnet Server Diagnostics

This section describes how to configure Telnet Server diagnostic parameters to customize the way the Technician Interface performs diagnostics on a router. Field Service personnel use these features to troubleshoot problems.

Enabling Diagnostic Reporting

This parameter allows field personnel to specify whether the Technician Interface displays a report that shows a record of all processing operations.

Site Manager: Diagnostic Report parameter: page A-11

Enabling Diagnostic Exercise

This parameter allows field personnel to enable exercise diagnostics on the Telnet Server.

Site Manager: Diagnostic Exercise parameter: page A-11

Enabling Diagnostic Network Data

This parameter allows you to specify whether you want the Technician Interface to display Telnet protocol information. It is used for diagnostic purposes only by field service personnel.

Site Manager: Diagnostic Network Data parameter: page A-11

Enabling Diagnostic PTY Data

This parameter lets you specify whether you want the Technician Interface to display pseudo-terminal driver (PTY) information.

Site Manager: Diagnostic PTY Data parameter: page A-12

Enabling Diagnostic Options

This parameter allows you to specify whether you want the Technician Interface to display information on Telnet options.

Site Manager: Diagnostic Options parameter: page A-12

Setting Technician Interface Login Scripts

This section describes the script files that run automatically when you log in. These scripts determine values for the Manager's Login, User's Login, and Force User Logout You can accept the defaults, or customize the scripts as needed.

Specifying a Filename for the Manager's Login Script

By default, the name of the Manager's script file is *automgr.bat*. You can specify a new name for the Manager's Login script by supplying an 8-character filename.

Site Manager: Manager's Login Script parameter: page A-12

Specifying a Filename for the User's Login Script

By default, the name of the User's Login script file is *autouser.bat*. You can specify a new name for the User's Login script file by supplying an 8-character filename. If you do not want to change the name of the User's Login script, accept the default name.

Site Manager: User's Login Script parameter: page A-7

Enabling and Disabling User Logout

By default, you can press control-c to cancel the user autoscript at login and access the Technician Interface.

Site Manager: Force User Logout parameter: page A-7

Changing the History File

You can determine the maximum number of Technician Interface commands you want stored in the local command history table. The table stores each command you enter at the Technician Interface prompt, on a first-in, first-out (FIFO) basis.

Site Manager: TI History Depth parameter: page A-13

Configuring the Telnet Client on the Router

After you create a Telnet Client on the router for outbound Telnet sessions, as described in Chapter 2, default values are in effect for all Telnet Client parameters (see parameter descriptions in Appendix A). You may want to change these parameter values, depending on the requirements of your network.

The following section describe information you supply and options you select that affect the way Telnet Client runs on the router.

Enabling Telnet Client on the IP Router

You can specify whether you want to enable or disable the Telnet Client for the IP router. By default, the Telnet Client on the IP router is enabled. This establishes outbound Telnet sessions from the Technician Interface to another router or to a UNIX station that supports Telnet. Select Disable to disable the Telnet Client on the IP router.

Site Manager: Enable/Disable parameter: page A-14

Enabling Verbose Debug Logging

You can specify whether you want the Technician Interface to enable or disable verbose debug logging. When you enable this parameter, you instruct the Technician Interface to display the negotiation process between the Telnet Server and Telnet Client. By default, verbose debug logging is off. This parameter is for diagnostic use only.

Site Manager: Verbose Debug Logging parameter: page A-14

Changing the Remote Port

You can change the default remote Telnet Server's TCP remote port by specifying a valid TCP port number.

Site Manager: Remote Port parameter: page A-15

Changing the Command Prompt

You can change the default Telnet Client command prompt by specifying any string less than 40 characters long.

Site Manager: Prompt parameter: page A-15

Where to Go Next

The following table shows you where to find additional information for configuring and customizing TCP, FTP, Telnet, and NTP.

For information on	Go to
TCP, FTP, Telnet, and NTP and how Bay Networks implements these protocols	Chapter 2
How to configure TCP services	Chapter 3
How to configure FTP services	Chapter 4
How to configure NTP services	Chapter 6
TCP, FTP, Telnet, and NTP parameter descriptions	Appendix A
TCP, FTP, Telnet, and NTP parameter default values	Appendix B

Chapter 6
Customizing NTP Services

This chapter describes how to create and customize NTP services. You should have read *Configuring Routers* or *Configuring Customer Access and Trunks (BNX Software)*, as appropriate for your platform, and have performed the following tasks:

1. **Opened a configuration file in local or remote mode**

1. **Selected the appropriate router type, specified a slot, and selected the link or net module that you want to insert in the slot (if you are using a local mode configuration file)**

2. **Configured IP on an interface using the default parameters, as described in Chapter 1**

3. **Verified that the time servers that you want to configure on the network are reachable via IP**

   To do this, you must *ping* the IP address of the time server you want to configure. If the server you want to configure is not on the local network, you will need to configure the appropriate IP routing protocol, such as RIP or OSPF. For information on pinging a server or configuring routing protocols, refer to *Configuring IP Services*.

4. **Created NTP in the Configuration Manager window**

You can create and enable NTP easily by using all the default parameter values that the Configuration Manager supplies.

If you decide to change some or all of the default parameters, refer to the instructions in this chapter. For a list of NTP parameters, see Appendix B.

Configuring NTP on the Router

The following sections describe information you supply and options you select that affect the way NTP runs on the router.

Enabling and Disabling NTP

After you create NTP on the router, as described in Chapter 1, default values are in effect for all NTP parameters (see parameter descriptions in Appendix A). You may want to change these values, depending on the requirements of your network.

Site Manager: Enable/Disable parameter: page A-15

Setting NTP Client Mode

There are three modes in which you can configure NTP: Unicast Client, Broadcast Client, and Multicast Client. By default, NTP runs in Unicast Client mode. Currently, Bay Networks supports only Client mode.

You select Unicast Client mode when you want to configure peers. You select Broadcast Client mode and Multicast Client mode when you want to configure access control filters to restrict certain peers from becoming time servers for an NTP client.

Site Manager: NTP Mode parameter: page A-16

Configuring Time Servers on a Router

You can configure time servers (peers) for time synchronization in Unicast Client mode only. Configuring a time server involves

- Adding time servers
- Specifying the configuration peer mode for the time server
- Setting the mode of operation of the router
- Specifying a source IP address
- Specifying peer preference
- Deleting peers

Adding Time Servers

You can add time servers to a router by specifying the IP address of each time server (peer). NTP adds the IP address of the time server to a peer list, which NTP uses when querying time servers for time information. Bay Networks recommends that you configure a minimum of three upper stratum time servers (peers) for a router, since it can apply an agreement algorithm to detect a problem on any part of the time source. You can, if necessary, add a maximum of five time servers on a router. Configuring multiple time servers ensures redundancy in case one peer goes down unexpectedly.

Site Manager: Peer IP Address parameter: page A-16

NTP queries all the time servers in the peer list for time information and then determines which server to synchronize its internal clock to based on the following criteria:

- Lowest stratum
- Closest in proximity to the primary time server
- Claimed highest precision

When the NTP client queries the time servers from the peer list, the servers respond with various time stamps, along with information about their clocks, such as stratum, precision, and time reference. The NTP client reviews a list of responses from all the available servers and chooses one server as the “best” time source from which to synchronize its internal clock.

Setting Config Peer Mode

The Config Peer Mode parameter allows you to specify the mode for the time server (peer). By default, Config Peer Mode is set to Server, indicating that the NTP client adjusts its clock to the given time server but does not attempt to adjust the time server’s clock. Currently, Bay Networks supports only the Server option.

Site Manager: Configure Peer Mode parameter: page A-18

Setting Local Host Mode

Local Host Mode indicates the mode of operation of the router (NTP client). By default, the Local Host Mode is set to Client, because only Unicast Client mode is supported.

Site Manager: Local Host Mode parameter: page A-18

Specifying the Source IP Address

The source IP address allows you to specify a single Internet protocol address that NTP uses to override the source address of the IP interface from which the NTP packet is transmitted. You use this parameter only when you want the time server to filter NTP time stamps for the NTP client based on IP source address. We recommend using a circuitless IP address as the source IP address.

You might also want to specify a source IP address when you have enabled security features on a time server and you want to restrict access to it.

Site Manager: Source IP Address parameter: page A-19

Specifying Peer Preference

The Peer Preference parameter allows you to specify a list of time servers (peers) that are preferred by the NTP client above and beyond the criteria for selecting peers (stratum setting, closest, and claimed higher precision).

By default, the Peer Preference option value is set to No. When this value is No, the NTP client can synchronize its internal clock to the “best” time source using the NTP decision criteria for selecting time servers.

To enable Peer Preference for a time server, you must change the Peer Preference option value to Yes. When the value is Yes, the NTP client synchronizes its internal clock to the preferred time server (peer).

Site Manager: Peer Preference parameter: page A-19

Deleting Time Servers from a Router

When you delete a time server (peer), NTP deletes from the peer list the IP address of that time server.

Configuring NTP Access Control

The access control feature allows you to selectively restrict NTP clients from receiving NTP time stamps from specific time servers on the network by filtering these time stamps. The filter is based on the source IP address or an IP subnet address. This is similar to an inbound filter that drops NTP packets based on source IP address and IP subnet mask.

Adding Access Control to a Time Server

To restrict an NTP server from receiving time stamps from specific time servers, you must specify the time server's IP address. NTP adds the IP address of the time server to an access control list, which the NTP client uses when querying time servers for time information. You use access control in Broadcast Client and Multicast Client mode.

Site Manager: Access IP Address parameter: page A-16

Specifying a Filter Type

By default, the filter type is set to Restrict, which tells NTP to drop specific NTP time stamps destined for an NTP client based on its source IP address and source subnet mask. For example, if you have ten time servers broadcasting to a router and you want to receive NTP time stamps from only three time servers, you can restrict the other seven time servers.

When you set the Filter Type to Prefer, NTP disables filtering on a specific time server's IP address or a range of time server's IP addresses.

Site Manager: Filter Type parameter: page A-17

Specifying an IP Subnet Mask

You can specify a IP subnet mask address to filter NTP time stamps based on a source subnet.

Site Manager: Access IP Mask parameter: page A-17

Deleting Access for a Time Server

When you delete access for a time server (peer), NTP removes from the access control list the IP address of the time server whose access you restricted.

Where to Go Next

The following table shows you where to find additional information for configuring and customizing TCP, FTP, Telnet, and NTP.

For information on	Go to
TCP, FTP, Telnet, and NTP and how Bay Networks implements these protocols	Chapter 2
How to configure TCP services	Chapter 3
How to configure FTP services	Chapter 4
How to configure Telnet services	Chapter 5
TCP, Telnet, FTP, and NTP parameter descriptions	Appendix A
TCP, Telnet, FTP, and NTP parameter default values	Appendix B

Appendix A
Parameter Descriptions

This appendix provides information on how you can edit, or customize, the parameters for the TCP, FTP, Telnet, and NTP interfaces you configure on the router. For each parameter you configure, this appendix provides the default setting, all valid parameter options, the parameter function, instructions for setting the parameter, and the management information base (MIB) object ID.

The Technician Interface allows you to modify parameters by issuing **set** and **commit** commands with the MIB object ID. This process is equivalent to modifying parameters using Site Manager. For more information about using the Technician Interface to access the MIB, refer to *Using Technician Interface Software*.

Caution: The Technician Interface does not verify the validity of your parameter values. Entering an invalid value can corrupt your configuration.

After you create TCP, FTP, Telnet, and NTP, you can edit the parameters for each of these protocols from the Configuration Manager window. For instructions on accessing this window, refer to *Configuring Routers* or *Configuring Customer Access and Trunks (BNX Software)*, as appropriate for your platform.

TCP Global Parameters

Use the following guidelines to configure TCP global parameters in the Configuration Manager window.

Parameter: Enable/Disable

Path: Protocols > Global Protocols > TCP > Global

Default: Enable

Options: Enable | Disable

Function: Enables or disables TCP on the router.

Instructions: Select Disable to disconnect from TCP. Also, you can select Disable if you do not need TCP, but want to access previous TCP statistics.

MIB Object ID 1.3.6.1.4.1.18.3.5.3.3.1.2

Parameter: Min. Retransmission Timeout (msec.)

Path: Protocols > Global Protocols > TCP > Global

Default: 250 milliseconds (ms)

Options: 100 through 15000 ms

Function: Sets the minimum value for the retransmission timeout. When one side of a TCP connection sends a frame and does not receive an acknowledgment from the other side of the connection within the timeout period, the sending station retransmits the frame.

Instructions: Specify the value you want to use for the minimum timeout period. If you are transmitting on a high-speed network and you set the parameter value too high, network performance may degrade because TCP must wait for the timeout period to elapse before retransmitting unacknowledged data.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.3.1.5

Parameter: **Max. Retransmission Timeout (msec.)**

Path: Protocols > Global Protocols > TCP > Global

Default: 240000 ms

Options: 15000 through ms

Function: Sets the maximum value for the retransmission timeout. When one side of a TCP connection sends a frame and does not receive an acknowledgment from the other side of the connection within the timeout period, the sending station retransmits the frame.

Instructions: Specify the value you want to use for the maximum timeout period. If you are transmitting on a low-speed network and you set the parameter value too low, the network may become congested as TCP retransmits unacknowledged frames that have not yet reached their destination.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.3.1.6

Parameter: **Max. Window Size (bytes)**

Path: Protocols > Global Protocols > TCP > Global

Default: 4096 bytes

Options: 512 through 65535 bytes

Function: Sets the maximum transmit-and-receive window size that TCP allows for each connection.

Instructions: Specify the window size. The larger the window size, the more memory each TCP connection consumes.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.3.1.18

FTP Global Parameters

Use the following guidelines to configure the parameters in the Edit FTP Global Parameters window.

Parameter: Enable/Disable

Path: Protocols > Global Protocols > FTP > Global
Default: Enable
Options: Enable | Disable
Function: Specifies whether the FTP subsystem is enabled or disabled.
Instructions: Specify Disabled if you want to disable FTP on the router.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.10.1.2

Parameter: Default Volume

Path: Protocols > Global Protocols > FTP > Global
Default: Volume 2
Options: Volume 1 to 13 | Volume A
Function: Specifies the number of the file system volume to which FTP writes transferred files and from which FTP retrieves files for transfer.
Instructions: On systems with a diskette, specify Volume A.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.10.1.3

Parameter: Login Retries

Path: Protocols > Global Protocols > FTP > Global
Default: 3 retries
Options: 0 through 5 retries
Function: Specifies the number of FTP login retries allowed after a login failure.
Instructions: Enter a value representing the number of login attempts that FTP will accept after a login failure before rejecting logins.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.10.1.4

Parameter: **Idle Time Out (secs)**

Path: Protocols > Global Protocols > FTP > Global

Default: 900 seconds

Options: 1 through 10000 sessions

Function: Specifies the length of time (in seconds) that FTP waits before closing an idle FTP control connection.

Instructions: Determine the maximum idle time you want to allow and specify the time value in seconds.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.10.1.5

Parameter: **Max. Sessions**

Path: Protocols > Global Protocols > FTP > Global

Default: 3 sessions

Options: 1 through 10000 sessions

Function: Specifies the maximum number of FTP sessions allowed at one time.

Instructions: Determine the maximum number of simultaneous sessions you want to allow and specify a value.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.10.1.6

Parameter: **Type of Service**

Path: Protocols > Global Protocols > FTP > Global

Default: Binary

Options: Binary | ASCII

Function: Specifies the current data transmission type.

Instructions: To transfer files consisting of ASCII characters, specify ASCII transmission. For non-ASCII files, specify Binary.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.10.1.7

Parameter: Control Connection

Path: Protocols > Global Protocols > FTP > Global
Default: Low Delay
Options: Normal | Low Delay
Function: Specifies the Type of Service value that FTP inserts in IP datagrams on a control connection.
Instructions: Choose the option that determines how the Internet transport layer handles datagrams on a control connection.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.10.1.8

Parameter: Data Transfer

Path: Protocols > Global Protocols > FTP > Global
Default: High Throughput
Options: Normal | High Throughput
Function: Specifies the Type of Service value that FTP inserts in IP datagrams on a data transfer connection.
Instructions: Choose the option that determines how the Internet transport layer handles datagrams on a data transfer connection.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.10.1.9

Parameter: TCP Window Size

Path: Protocols > Global Protocols > FTP > Global
Default: 16000 bytes
Range: 5000 to 64000 bytes
Function: Specifies the size of the windows used for TCP connections.
Instructions: Determine the window size you require and specify the size in bytes.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.10.1.10

Telnet Configuration Parameters

Use the following guidelines to configure the Telnet configuration parameters in the Configuration Manager window.

Parameter: Manager's Login Script

Path: Protocols > Global Protocols > Telnet > Global

Default: *automgr.bat*

Options: The name of the manager's login script file

Function: At login, executes the manager's login script file automatically.

Instructions: If you did not change the name of the manager's login script file, accept the default. Otherwise, enter the new name (must be eight characters or less).

MIB Object ID. 1.3.6.1.4.1.18.3.5.3.7.1.21

Parameter: User's Login Script

Path Protocols > Global Protocols > Telnet > Global

Default: *autouser.bat*

Options: None

Function: At login, executes the user's login script file automatically.

Instructions: If you did not change the name of the user's login script file, accept the default. Otherwise, enter the new name (must be eight characters or less).

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.7.1.22

Parameter: Force User Logout

Path: Protocols > Global Protocols > Telnet > Global

Default: Disable

Options: Enable | Disable

Function: Specifies whether the user can press control-c to cancel a user autoscript at login (when a user autoscript is in effect).

Instructions: Select Enable to prevent using control-c to cancel the user autoscript at login. Select Disable to allow the user to press control-c to cancel the user autoscript at login.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.7.1.23

Telnet Server Global Parameters

Use the following guidelines to configure the Telnet global parameters in the Edit Telnet Server Global Parameters window.

Parameter: Enable/Disable

Path: Protocols > Global Protocols > Telnet Server > Global

Default: Disable

Options: Enable | Disable

Function: Specifies whether Telnet is enabled for the IP router, allowing you to establish incoming Telnet sessions to the Technician Interface.

Instructions: Select Enable to enable Telnet for the IP router. Select Disable to disable Telnet for the IP router.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.7.1.2

Parameter: TI Lines per Screen

Path: Protocols > Global Protocols > Telnet Server > Global

Default: 24 lines

Options: 1 through 24 lines

Function: Specifies the maximum number of lines displayed on the Telnet Technician Interface console screen. The screen may override the number of lines you specify if Telnet can negotiate the window size with the remote client.

Instructions: Set according to your console requirements.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.7.1.3

Parameter: **TI More**

Path: Protocols > Global Protocols > Telnet Server > Global

Default: Enable

Options: Enable | Disable

Function: Specifies whether the Technician Interface pauses after each screen fills with data.

Instructions: Select Enable to configure the Technician Interface to pause after each screen fills with data. Select Disable to configure the Technician Interface not to pause after each screen fills with data.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.7.1.4

Parameter: **TI Prompt**

Path: Protocols > Global Protocols > Telnet Server > Global

Default: None

Range: 1 to 18 alphanumeric characters

Function: Specifies the character string used as the login prompt on the Telnet Technician Interface console screen.

Instructions: Specify a character string.

Site Manager disconnects the current session if you modify the TI Prompt parameter.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.7.1.5

Parameter: **Login Timeout (min.)**

Path: Protocols > Global Protocols > Telnet Server > Global

Default: 1 minute

Options: 1 through 99 minutes (99 = infinity)

Function: Specifies the number of minutes that can elapse before the Technician Interface disconnects the Telnet session if you do not enter a login ID at the login prompt.

Instructions: Accept the default value (1 minute) or specify a different value.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.7.1.6

Parameter:	**Password Timeout (min.)**
Path:	Protocols > Global Protocols > Telnet Server > Global
Default:	1 minute
Options:	1 through 99 minutes (99 = infinity)
Function:	Specifies the number of minutes that can elapse before the Technician Interface disconnects the Telnet session if you do not enter a password at the password prompt.
Instructions:	Accept the default value (1 minute) or specify a different value.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.7.1.7

Parameter:	**Command Timeout (min.)**
Path:	Protocols > Global Protocols > Telnet Server > Global
Default:	15 minutes
Range:	1 through 99 minutes (99 = infinity)
Function:	Specifies the number of minutes that can elapse before the Technician Interface disconnects the Telnet session if you do not enter a command at the command prompt.
Instructions:	Accept the default value (15 minutes) or specify a different value.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.7.1.8

Parameter:	**Login Retries**
Path:	Protocols > Global Protocols > Telnet Server > Global
Default:	3 login attempts
Options:	1 through 99 login attempts
Function:	Specifies the maximum number of login attempts you can make before the Technician Interface disconnects the Telnet session.
Instructions:	Accept the default value (3) or specify a different value.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.7.1.9

Parameter: Diagnostic Report

Path: Protocols > Global Protocols > Telnet Server > Global
Default: Disable
Options: Enable | Disable
Function: Specifies whether the Technician Interface displays a record of all processing operations. Used for diagnostic purposes only.
Instructions: Accept the default (Disable). This parameter is for field service personnel only.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.7.1.15

Parameter: Diagnostic Exercise

Path: Protocols > Global Protocols > Telnet Server > Global
Default: Disable
Options: Enable | Disable
Function: Used for diagnostic purposes only.
Instructions: Accept the default (Disable). This parameter is for field service personnel only.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.7.1.16

Parameter: Diagnostic Network Data

Path: Protocols > Global Protocols > Telnet Server > Global
Default: Disable
Options: Enable | Disable
Function: Specifies whether the Technician Interface displays Telnet protocol information. Used for diagnostic purposes only.
Instructions: Accept the default (Disable). This parameter is for field service personnel only.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.7.1.17

Parameter: Diagnostic PTY Data

Path: Protocols > Global Protocols > Telnet Server > Global
Default: Disable
Options: Enable | Disable
Function: Specifies whether the Technician Interface displays pseudo-terminal driver (PTY) information. Used for diagnostic purposes only.
Instructions: Accept the default (Disable). This parameter is for field service personnel only.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.7.1.18

Parameter: Diagnostic Options

Path: Protocols > Global Protocols > Telnet Server > Global
Default: Disable
Options: Enable | Disable
Function: Specifies whether the Technician Interface displays Telnet options information. Used for diagnostic purposes only.
Instructions: Accept the default (Disable). This parameter is for field service personnel only.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.7.1.19

Parameter: Manager's Login Script

Path: Protocols > Global Protocols > Telnet Server > Global
Default: *automgr.bat*
Options: The name of the manager's login script file.
Function: At login, executes the manager's login script file automatically.
Instructions: If you did not change the name of the manager's login script file, accept the default. Otherwise, enter the new name (must be eight characters or less).
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.7.1.21

Parameter: **User's Login Script**

Path: Protocols > Global Protocols > Telnet Server > Global

Default: *autouser.bat*

Options: The name of the user's login script file.

Function: At login, executes the user's login script file automatically.

Instructions: If you did not change the name of the user's login script file, accept the default. Otherwise, enter the new name (must be eight characters or less).

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.7.1.22

Parameter: **Force User Logout**

Path: Protocols > Global Protocols > Telnet Server > Global

Default: Disable

Options: Enable | Disable

Function: Specifies whether the user can press control-c to cancel a user autoscript at login (when a user autoscript is in effect).

Instructions: Set the parameter to Enable to prevent using control-c to cancel the user autoscript at login.
Set the parameter to Disable to allow the user to press control-c to cancel the user autoscript at login.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.7.1.23

Parameter: **TI History Depth**

Path: Protocols > Global Protocols > Telnet Server > Global

Default 20

Options: 1 to 40 commands

Function: Specifies the maximum number of Technician Interface commands stored in the local command history table. The table stores each command you enter at the Technician Interface prompt, on a first-in, first-out (FIFO) basis.

Instructions: Set the maximum number of commands that you want the router to store, for subsequent recall with the Technician Interface **history** command.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.7.1.24

Telnet Client Global Parameters

Use the following guidelines to configure the global parameters in the Edit Telnet Client Global Parameters window.

Parameter: Enable/Disable

Path: Protocols > Global Protocols > Telnet Client > Global

Default: Enable

Range: None

Function: Specifies whether the Telnet Client is enabled for the IP router, allowing you to establish outbound Telnet sessions from the Technician Interface to another router or to a UNIX station that supports Telnet.

Instructions: Select Enable to enable Telnet Client for the IP router or Disable to disable it.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.7.2.2

Parameter: Verbose Debug Logging

Path: Protocols > Global Protocols > Telnet Client > Global

Default: OFF

Options: ON | OFF

Function: Specifies whether the Technician Interface displays the negotiation process between the Telnet Server and Telnet Client. This parameter is for diagnostic use only.

Instructions: Select ON to enable verbose debug logging or OFF to disable it.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.7.2.3

Parameter: **Remote Port**
Path: Protocols > Global Protocols > Telnet Client > Global
Default: 23
Options: Any valid TCP port number.
Function: Specifies the default remote Telnet Server's TCP port.
Instructions: Enter the appropriate value for the default remote Telnet Server's TCP port.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.7.2.4

Parameter: **Prompt**
Path: Protocols > Global Protocols > Telnet Client > Global
Default: None
Options: Any text string less than 40 characters long
Function: Specifies the default Telnet Client command prompt.
Instructions: Enter any text string less than 40 characters long; for example, Router1%
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.7.2.5

NTP Global Parameters

Use the following guidelines to configure NTP parameters.

Parameter: **Enable/Disable**
Path: Select Protocols > Global Protocols > NTP > Global
Default: Enable
Options: Enable | Disable
Function: Enables or disables the NTP Subsystem on the router.
Instructions: To disable the NTP Subsystem on the router, specify Disable and click on OK in the Edit NTP Global Parameters window.
MIB Object ID: 1.3.6.1.4.1.1.18.3.5.3.17.1.1.3

Parameter: NTP Mode

Path: Protocols > Global Protocols > NTP > Global

Default: Client

Options: Client, BClient, or MClient

Function: Specifies the mode in which you want NTP to run on your router.

Instructions: Specify either Unicast Client (Client), Broadcast Client (BClient), or Multicast Client (MClient) mode and click on OK in the Edit NTP Global Parameters window.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.17.1.1.4

Parameter: Peer IP Address

Path: Protocols > Global Protocols > NTP > Add Peers

Default: None

Options: 0.0.0.0 or any valid IP address

Function: Specifies the IP address of the time server (peer) you want to configure. NTP adds the IP address of the time server to a peer list. NTP uses this peer list when querying time servers for time information to determine the best time server to synchronize its internal clock.

Instructions: Specify the IP address of the time server (peer) you want to configure in the NTP Peer Configuration window.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.17.3.1.6

Parameter: Access IP Address

Path: Protocols > Global Protocols > NTP > Access > Add Access

Default: None

Options: 0.0.0.0 or any valid IP address

Function: Allows you to configure the source IP address of the time server whose access to the NTP client you want to restrict.

Instructions: Enter the IP address of the time server whose access you want to restrict in the NTP Access Configuration window.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.17.2.1.3

Parameter: **Filter Type**

Path: Protocols > Global Protocols > NTP > Access

Default: Restrict

Options: Restrict | Prefer

Function: Specifies that you want to restrict specific time servers from sending NTP packets to the NTP client. The NTP client will filter packets from a time server whose IP address you have restricted based on its source IP address and source subnet mask.

Instructions: Specify Restrict or Prefer in the Filter Type Selection box.

When you specify Prefer, NTP disables filtering on a specific time server's IP address or a range time server's IP addresses.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.17.2.1.2

Parameter: **Access IP Mask**

Path: Select Protocols > Global Protocols > NTP > Access

Default: None

Options: 0.0.0.0 or any valid IP address

Function: Specifies a IP subnet mask address to filter NTP time stamps based on a source subnet. NTP drops all packets sent from a specific time server on a specified subnet.

Instructions: Specify the IP subnet mask address of the filter in the IP Mask Selection box in the NTP Access Configuration window.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.17.2.1.4

Parameter:	**Configure Peer Mode**
Path:	Select Protocols > Global Protocols > NTP > Peers.
Default:	Server
Options:	Server only
Function:	Specify the mode for the time server (peer). By default, Config Peer Mode is set to Server.
Instructions:	To configure a time server (peer), click on Add Peer and specify the peer's IP address. Bay Networks currently supports only the Server option.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.17.3.1.3

Parameter:	**Local Host Mode**
Path:	Select Protocols > Global Protocols > NTP > Peers
Default:	Client
Options:	Client
Function:	Allows you to specify the local mode in which you want to configure the NTP client. Currently, Bay Networks supports only Unicast Client mode.
Instructions:	Specify Unicast Client mode in the Configuration Peer Mode selection box.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.17.3.1.5

Parameter: **Source IP Address**

Path: Select Protocols > Global Protocols > NTP Peers

Default: None

Options: Any valid IP address

Function: Allows you to specify a single Internet protocol address that NTP uses to override the source address of the interface from which the NTP packet is transmitted. You use this parameter only when you want the time server to filter NTP packets based on IP source address. We recommend using a circuitless IP address as the source IP address.

If you do not specify a source IP address, NTP uses the IP address of the outbound router IP interface address.

Instructions: Specify the source IP address of a time server in the Source IP Address selection box.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.17.3.1.7

Parameter: **Peer Preference**

Path: Select Protocols > Global Protocols > NTP > Peers

Default: No

Options: Yes | No

Function: Allows you to specify which time server (peer) you want to be preferred by the NTP client.

Instructions: When you select Yes, the NTP client synchronizes its internal clock only preferred time servers (peer) using the decision criteria (stratum setting, closest, and claimed higher precision).

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.17.3.1.8

Appendix B
Site Manager Default Settings

This appendix lists the Site Manager default settings for TCP, FTP, Telnet, and NTP. Use the Configuration Manager to edit any of the Site Manager default settings listed here.

TCP Parameters

Table B-1 lists the default parameter settings for TCP.

Table B-1. TCP Configuration Parameters

Parameter	Default
Enable/Disable	Enable
Min. Retransmission Timeout	250 ms
Max. Retransmission Timeout	240000 ms
Max. Window Size	4096 bytes

FTP Parameters

Table B-2 lists the Site Manager default parameter settings for the File Transfer Protocol (FTP).

Table B-2. FTP Configuration Parameters

Parameters	Default
Enable/Disable	Enable
Default Volume	Volume 2
Login Retries	3 retries
Idle Time Out	900 seconds
Max. Sessions	3 sessions
Type of Service	Binary
Control Connection	Low delay
Data Transfer	High Throughput
TCP Window Size	16000 bytes

Telnet Parameters

Table B-3 and Table B-4 list the Site Manager default parameter settings for Telnet.

Table B-3. Telnet Server Configuration Parameters

Parameters	Default
Enable/Disable	Enable
TI Lines per Screen	24 lines
TI More	Enable
TI Prompt	None
Login Timeout	1 minute
Password Timeout	1 minute
Command Timeout	15 minutes
Login Retries	3 login attempts
Diagnostic Report	Disable
Diagnostic Exercise	Disable
Diagnostic Network Data	Disable
Diagnostic PTY Data	Disable
Diagnostic Options	Disable
Manager's Login Script	*automgr.bat*
User's Login Script	*autouser.bat*
Force User Logout	Disable
TI History Depth	20 commands

Table B-4. Telnet Client Configuration Parameters

Parameters	Default
Enable/Disable	Enable
Verbose Debug Logging	OFF
Remote Port	23
Prompt	None

NTP Parameters

Table B-5 lists the Site Manager default parameter settings for the Network Time Protocol (NTP).

Table B-5. NTP Configuration Parameters

Parameters	Default
Enable/Disable	Enable
NTP Mode	Unicast Client
Create/Delete Peer	Create
Configure Peer Mode	Server
Local Host Mode	Client
Source IP Address	None
Peer Preference	No
Access IP Address	None
Filter Type	Restrict
Access IP Mask	None
Peer IP Address	None

Index

A

Acknowledgment with retransmission, 2-3

B

Bay Networks
- CompuServe forum, xvii, xxvi
- Customer Service FTP, xxv
- customer support, xvii
- Home Page on World Wide Web, xviii
- home page on World Wide Web, xxv
- InfoFACTS service, xviii, xxvii
- publications, ordering, xx
- support programs, xxiv
- Support Source CD, xxvi
- Technical Response Center, xviii, xxiii, xxvii
- technical support, xxiii

BGP parameters, global
- BGP Identifier, A-4, A-5, A-6, A-14, A-15, A-16, A-17

C

Caching, 2-3

Checksums, 2-3

Clients, 2-4, 2-7

Command Timeout parameter, A-10

CompuServe, Bay Networks forum on, xvii, xxvi

Connections, 2-4

Customer Service FTP, xxv

customer support. *See* getting help

E

Enable/Disable, A-14, A-15

F

Flow control, 2-3, 2-7

FTP Global parameters
- Enable/Disable, A-4
- Idle Time Out, A-5
- Login Retries, A-4

G

Getting help
- from a Bay Networks Technical Response Center, xviii, xxvii
- from the Support Source CD, xxvi
- through CompuServe, xvii, xxvi
- through Customer Service FTP, xxv
- through InfoFACTS service, xviii, xxvii
- through World Wide Web, xviii, xxv

I

Idle Time Out parameter, A-5

Inbound Telnet, 2-12
- *See also* Telnet Server

InfoFACTS service, xviii, xxvii

Internet Protocol (IP), 2-1, 2-2

M

Max. Retransmission Timeout parameter, A-3

Memory and number of Telnet connections, 2-12

considerations for configuring TCP, 2-5
Min. Retransmission Timeout parameter, A-2

O

Outbound Telnet, 2-11
See also Telnet Client
Out-of-order caching, 2-3

P

Parameters, *See*
Command Timeout
Enable/Disable
Idle Time Out
Max. Retransmission Timeout
Min. Retransmission Timeout
Ports, 2-4

R

Reference material, 3-3

S

Sequence numbers, 2-3
Simple Network Management Protocol (SNMP), 2-11
Sockets, 2-4
Support Source CD, xxvi

T

TCP
clients, 2-4, 2-6
connection states, 2-4 to 2-7
connections for, 2-4
memory considerations, 2-5
overview of, 2-2 to 2-7
ports, 2-4
TCP Global parameters, A-2 to A-3
descriptions of, A-2 to A-3
Enable/Disable, A-2
Max. Retransmission Timeout, A-3
Max. Window Size, 2-5, A-3, A-7, A-8
Min. Retransmission Timeout, A-2
Technician Interface, 2-11
Telnet, 2-6 to 2-11
Telnet Client, 2-6
parameter descriptions for, A-14 to A-15
Telnet Client Global parameters
Enable/Disable, A-14, A-15
Remote Port, A-15
Verbose Debug Logging, A-14
Telnet configuration parameters
Force User Logout, A-7
Manager's Login Script, A-7, A-8
Telnet Server Global parameters
Command Timeout, A-10
Diagnostic Network Data, A-11
Diagnostic Options, A-12
Diagnostic Report, A-11
Force User Logout, A-13
Login Retries, A-10
Login Timeout, A-9, A-10
TI More, A-9
User's Login Script, A-13
Transmission Control Protocol. *See* TCP

W

Window size for TCP, 2-5, 4-4, A-6
World Wide Web, Bay Networks Home Page on, xviii
World Wide Web, Bay Networks home page on, xxv